TU Clausthal

Bachelor-, Master- und Doktorandenseminar
des Instituts für Informatik

Language Independent Security Analysis for Injection Attacks

Malte Mues, B.Sc., TU Clausthal

Due to current trends in information systems like cloud computing and the Internet of Things (IoT), information security gains increasing attention. Network boundaries are dissolved by new business strategies such as “bring your own device to work”. Therefore it is mandatory to rethink information system design and focus more on secure implementations instead of outer system protection. This raises the question how individualized constraints regarding the information system security are formulated and checked on the system’s implementation over the life cycle. The presented master’s thesis focus on one possibility to answer this question for injection attacks especially SQL injection and command line injection.

Previous work at the TU Clausthal by Herold[1] demonstrates, how architectural constraints can be enforced to protect architecture erosion over time. The source code and the constraints description is transformed into a logical representation first to analyze compliance in the logical representation consecutively. As the methodology is designed to analyze architectural constraints, it just focus on the structural elements from a language like classes and interfaces during the transformation. The presented thesis extends the existing concept towards data flow analysis in a first step. In connection, it is outlined how data flow may be used to detect information flow weaknesses that allow SQL or command injection attacks. For that purpose taint marking is applied on top of the data flow. The thesis is completed by a proof of concept implementation showing feasibility of the previously described taint analysis. The concept is evaluated and discussed using a few selected examples from the OWASP Security Benchmark[2].

[1] Sebastian Herold. *Architectural Compliance in Component-Based Systems*. Dissertation, Clausthal University of Technology, 2011.

[2] Owasp benchmark for security automation. https://www.owasp.org/index.php/Benchmark#tab=Main. Accessed: 2016-05-03

Freitag, den 10.06.2016, 16 Uhr s.t. im Seminarraum 124, IfI, Arnold-Sommerfeld-Straße 1

Technische Universität Clausthal • Institut für Informatik • Julius-Albert-Straße 4 • 38678 Clausthal-Zellerfeld
Tel +49.(0)5323.72.7100 • Fax +49.(0)5323.72.7139 • http://www.in.tu-clausthal.de • info@in.tu-clausthal.de